Department of the Army
Pamphlet 25–2–2

Information Management: Army Cybersecurity

Cybersecurity Tools Unified Capabilities Approved Products List Process

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25–2–2
Cybersecurity Tools Unified Capabilities Approved Products List Process

This administrative revision, dated 1 November 2022—

- Changes proponency from CIO/G–6 to Deputy Chief of Staff, G–6 (title page).

This new pamphlet, dated 8 April 2019—

- Provides guidance for the vetting, approval, acquisition, and use of cybersecurity tools (cybersecurity and cybersecurity-enabled products) within the Department of the Army (chap 2).

- Provides guidance for Army use of the Department of Defense Unified Capabilities Approved Products List (chap 3).

- Amplifies procedures and guidance found in DODI 8100.04 (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–2

Information Management: Army Cybersecurity

Cybersecurity Tools Unified Capabilities Approved Products List Process

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This pamphlet provides guidance for the vetting, approval, acquisition, and use of cybersecurity tools.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Deputy Chief of Staff, G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Appendixes

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose
This pamphlet provides guidance for the vetting, approval, acquisition, and use of cybersecurity tools (cybersecurity and cybersecurity-enabled products) within the Department of the Army (DA), and leverages applicable Department of Defense (DOD) and DA publications. It contains amplifying procedures and guidance to AR 25–2, DODI 8100.04, and the Army's use of the DOD Unified Capabilities (UC) Approved Products List (APL). This pamphlet also addresses the process for placing cybersecurity tools on the DOD UC APL and explains the roles and duties within the DOD UC APL process. The DOD UC APL process provides for an increased level of confidence through cybersecurity and interoperability certification.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Applicability
This pamphlet applies to cybersecurity tools used in the Army for strategic, operational, and tactical network environments. It does not apply to the vetting processes of open source technologies, cross domain solutions, protected distributed systems, communications security technologies requiring National Security Agency approved key management (such as suite A and suite B),and enterprise mandated security capabilities such as Assured Compliance Assessment Solution, Host Based Security System, and end user devices.

1–5. Transition to the Department of Defense Unified Capabilities Approved Products List process
Effective 1 October 2010, the Chief Information Officer, G–6 (CIO/G–6) mandated the use of the DOD UC APL, and discontinued the Army Information Assurance (IA) APL.

a. Established in accordance with the DOD Unified Capabilities Requirements (UCR) 2013, Change 1 (UCR 2013, Change 1), the DOD UC APL process was developed in accordance with DODI 8100.04 and is managed by the Defense Information Systems Agency (DISA) Network Services Unified Capabilities Certification Office (UCCO). Use of the DOD UC APL allows DOD components to purchase and operate UC systems over all DOD network infrastructures (see DODI 8100.04).

b. Per AR 25–2, the Army will use the DOD UC APL when purchasing all security-related hardware, firmware, and software components (excluding cryptographic modules). On 30 September 2010, all approved products on the Army IA APL were validated and fast tracked to the DOD UC APL.

c. The CIO/G–6 Cybersecurity Directorate, Tools and Assessments Branch, usarmy.pentagon.hqda-cio-g-6.mbx.cyber-ia-tools@mail.mil is the appropriate contact for all questions and concerns regarding the Army's use of the DOD UC APL tools assessments process.

Chapter 2
Requirements

2–1. Vetting and approval requirements
Evaluate and validate all cybersecurity tools used in the Army for strategic, operational, and tactical network environments in accordance with AR 25–1, AR 25–2, DODI 8100.04, DOD UCR, and guidance from:

a. The National Information Assurance Partnership (NIAP) Evaluation and Validation Program.

(1) The following DOD UC APL products must be NIAP-certified or proven to be in the NIAP certification process prior to being placed on the UC APL:

(a) Firewall.

(b) IA Tool.

(c) Internet Protocol Count.

(d) Intrusion Prevention System.

(e) Integrated Security Solution.

(f) Network Access Controller.

(g) Virtual Private Network – concentrator.

(h) Wireless Intrusion Detection System.

(2) Some products may not require NIAP validation because an applicable NIAP protection profile has not been developed. However, in all cases, vendors will contact NIAP directly (https://www.niap-ccevs.org/) to determine the appropriate way forward for their products in the NIAP certification process, if applicable.

b. The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 140–2 (FIPS 140–2) Validation Program.

(1) All cybersecurity tools using encryption modules for the protection of Army information will use encryption modules that are FIPS 140–2 validated at the appropriate security levels. The authorizing official (AO) in each organization must ensure that computer and telecommunication systems utilizing cryptographic modules provide an acceptable level of security for the given application and environment.

(2) The product(s) can begin evaluation without FIPS approval, provided that the cryptographic module is already in process for evaluation at an accredited FIPS Cryptographic Module Validation Program laboratory. The product(s) will not be placed on the DOD UC APL until the module is FIPS 140–2 compliant. In cases of version and design changes to the module, the vendor must submit the module to NIST for an impact assessment on the existing FIPS validation. NIST will determine if changes to an encryption module will require a new FIPS validation. For certain technologies that provide end-to-end encryption, such as an internet protocol security virtual private network, the vendor must obtain two separate FIPS certificates, one for the client and one for the server.

2–2. Acquisition and use requirements

a. As stated in AR 25–2, all security-related hardware, firmware, and software components (excluding cryptographic modules) required to protect information systems will be acquired in accordance with public law and will have been evaluated and validated in accordance with appropriate criteria, schemes, or protection profiles (https://www.niap-ccevs.org/) and this pamphlet. Cybersecurity tools listed on the DOD UC APL at https://aplits.disa.mil/processaplist.action will be evaluated/selected first, and then procured through the Project Director, Computer Hardware and Enterprise Software Solutions (CHESS) contract vehicles before other cybersecurity products are procured. CIO/G–6 may approve exceptions (forward requests to usarmy.pentagon.hqda-cio-g-6.mbx.cyber-ia-tools@mail.mil) to cybersecurity products evaluations when no criteria, protection profile, or schema exists or is under development, and the removal or prohibition of such a cybersecurity tool would significantly degrade or reduce the ability of personnel to secure, manage, and protect the infrastructure.

b. Procure all approved cybersecurity tools through CHESS. Before purchasing a product, coordinate with the local Network Enterprise Center to ensure the product complies with policy and is authorized to connect to the DOD Information Network. Cybersecurity tools procured for closed or restricted systems must be coordinated with the organization's Information Systems Security Manager prior to purchase. Connecting to the network will require approval from the cognizant AO.

c. The Army will follow the guidelines below to acquire and use cybersecurity tools:

(1) Exercise due diligence in the planning and pre-acquisition strategy of cybersecurity technology at the initiation phase of system design and development, as well as throughout the system life cycle.

(2) Procure approved products with the exact hardware models, firmware, and software release versions listed on the DOD UC APL. If a specific product, version, and function are not published on the DOD UC APL, it has not been approved or vetted.

(3) Verify end of life, end of sale, and/or end of support by the manufacturer before purchase. The UC APL identifies these products as “End of Sale” (see the DOD UC APL Removal List at http://www.disa.mil/services/network-services/ucco/apl-removal-list).

(4) Products with expired certifications/removed from UC APL are no longer approved for purchase. However, products procured prior to UC APL removal may be eligible for continued operation in DOD networks provided applicable security requirements are met (information assurance vulnerability alert, Security Technical Implementation Guide (STIG), and so forth). In such cases, vendor end of life, and end of support (software/hardware) must be taken into account prior to product use. Organizations are encouraged to update to an approved capability as an expired capability will affect future accreditation status.

(5) Products are certified for 3 years through the DOD UC APL process. To obtain certification information for products listed on the DOD UC APL, select the “Product Info" tab next to the product in question. The certification information is listed under the statement, “This product is certified for the following device type(s).”

Chapter 3
Department of Defense Unified Capabilities Approved Products List processes, roles, and duties

3–1. Department of Defense Unified Capabilities Approved Products List process rules and guiding principles

a. To add a cybersecurity tool to the DOD UC APL, follow the procedures and guidance indicated in figure 3–1 and prescribed in the DOD UC APL Process Guide at http://www.disa.mil/~/media/files/disa/services/ucco/apl-process/ucapl_process.pdf.

b. UCCO is the DISA staff element that manages the DOD UC APL. UCCO provides process guidance, coordination, information, and support to Government sponsors and vendors throughout the entire process, from registration to attainment of DOD UC APL status. In addition, UCCO manages the DOD UC APL Removal List, which consists of products that have been removed from the DOD UC APL. As the DOD moves toward a distributed testing environment, UCCO will be the primary point of contact for scheduling and coordinating partnering test laboratories.

c. To list a product on the DOD UC APL, follow these procedures:

(1) A Government representative must sponsor the product. Two Government points of contact are required to ensure sponsor availability for attending initial contact meetings (ICMs) and out-briefs.

(2) UCCO sends a verification request to the Government representative to confirm he or she—

(a) Agrees to be the Government sponsor of the submitted product.

(b) Agrees to attend the ICM and out-brief.

(c) Agrees to the configuration submitted by the vendor.

(3) The sponsor approves solution under test configuration.

(4) UCCO issues a tracking number for product submissions and schedules the ICM. The outcome of the ICM will be the determination of a Joint Interoperability Test Command (JITC) action officer, the APL product type, the business model, cybersecurity/interoperability requirements, and the testing laboratory.

(5) The assigned JITC action officer will coordinate the business model with the vendor.

(6) Cybersecurity/interoperability testing is completed.

(7) The Army certification authority (CA) completes the certification determination recommendation letter and returns it to UCCO. UCCO posts the approved product information on the DOD UC APL website (https://aplits.disa.mil).

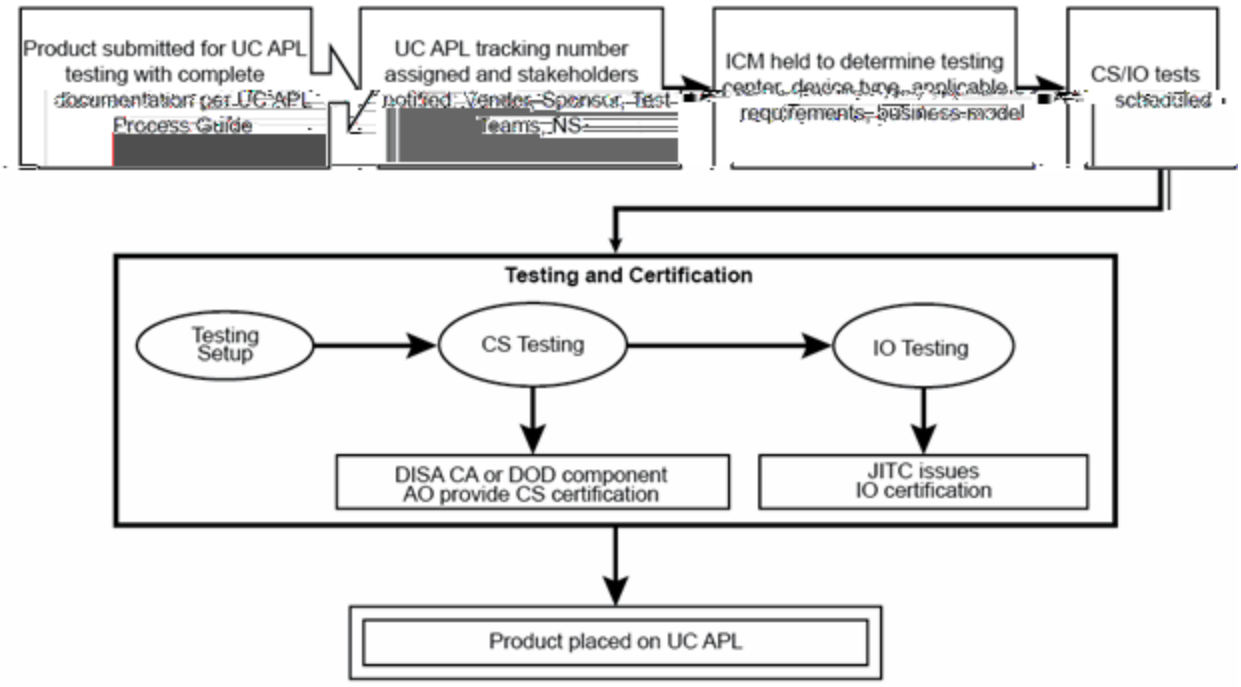

Figure 3–1. Standard process for Department of Defense Unified Capabilities Approved Products List certification

d. In cases where the DISA CA or DOD component CA issues a negative cybersecurity certification recommendation letter, UCCO will notify the vendor. UCCO allows 10 business days for the vendor to address and correct outstanding issues in the cybersecurity report. If the vendor fails to resubmit corrections to the UCCO within this timeframe, the tracking number is retired and the vendor must reinitiate the UC APL process. If the vendor corrects the report, mitigates, or resolves the findings and submits valid plan of action and milestones (POA&Ms), UCCO will resubmit the report to DISA CA or DOD component CA with a request for reconsideration of the certification recommendation.

3–2. Desktop review process

For any changes to a product that is already on the DOD UC APL, including patch updates and POA&M closure, contact the UCCO via the DOD UC APL website (https://aplits.disa.mil) to request a desktop review. The desktop review application will be reviewed by UCCO, which will decide which of the following is required: an update to the APL memorandum, minimal testing using the same tracking number, or a new submission for testing resulting in new tracking number. New software releases must be submitted to UCCO using the same process as a new submission. Adhere to the following procedures to submit a desktop review:

a. The vendor requests a desktop review via the DOD UC APL website (https://aplits.disa.mil). In addition, the vendor must provide a detailed description of the change to be evaluated within 5 business days of the desktop review request.

b. UCCO validates the request against desktop review criteria.

c. UCCO sends desktop review information and documentation to the testing laboratory that performed the original product cybersecurity/interoperability testing.

d. The testing laboratory will designate an action officer to coordinate an initial cybersecurity/interoperability review within 5 business days. This action officer will present one of the following recommendations to UCCO:

(1) *No testing is recommended.* The only recommendation is to update the DOD UC APL memorandum. The laboratory will provide a concise, detailed description/justification for this recommendation.

(2) *Minimal testing is recommended.* The laboratory will provide a concise, detailed description/justification for this recommendation.

(3) *New submission is recommended.* The laboratory will provide a concise, detailed description/justification for this recommendation.

e. If UCCO determines the desktop review application to be applicable, UCCO will forward the testing laboratory's recommendation to the capabilities center for review and coordination with a service manager. The capabilities center has 3 business days to provide—

(1) Concurrence or non-concurrence on the testing laboratory's recommendation.

(2) If the cybersecurity posture of the product is changed, the original CA for the product will be contacted in parallel with the capabilities center. This could be the Service CA for products that Service sponsored or DISA Field Security Operations.

f. JITC updates the interoperability certification letter.

g. Upon receipt of an updated interoperability certification letter from JITC, UCCO updates the product's cybersecurity assessment package and posts the updated product information on the DOD UC APL website (https://aplits.disa.mil).

3–3. Department of Defense Unified Capabilities Approved Products List fast track process

The DOD UC APL fast track process intends to expedite the addition of products to the DOD UC APL. The DOD UC APL fast track process is structured to deal with the fact that DOD sponsors have a need for products for which they have reasonably well-established requirements and, in some cases, test results. Yet these products may not appear in the DOD UCR that is published on an annual basis. If the UC steering group agrees that new product categories and/or new products should be added to the DOD UCR, the DOD sponsors and vendors will not have to wait for the next version of the DOD UCR to get them tested and placed on the DOD UC APL. DOD UC APL testing can begin based on existing requirements that will be placed in the next version of the DOD UCR.

a. Products that are candidates for the DOD UC APL fast track process are—

(1) Products that have well-established requirements within existing DOD UCR product categories. In some cases, the existing requirements can be augmented by current DOD UCR requirements.

(2) Products that have existing test results that can be reused to verify requirements against current DOD UCR products or approved DOD UC APL products.

(3) Products that are fielded in operational networks and successfully perform from both a cybersecurity and interoperability perspective.

(4) Products that should be added to the DOD UCR per the UC steering group.

b. The three categories of DOD UC APL fast track products are—

(1) *Products within current DOD UCR product categories.* This category includes products that were tested by JITC before development of the product category or products that have existing requirements similar to those in the DOD UCR that can be augmented with DOD UCR requirements.

(2) *Products that are operationally validated.* This category includes products that are currently operating in DOD networks that have an AO-signed approval to operate, are in compliance with appropriate STIGs, and are requesting DOD UC APL status. Products may be end of life (that is, retired DOD UC APL status) or active (that is, normal DOD UC APL status).

(3) *New DOD UCR product categories.* This category includes products that have existing requirements that can be used in the next version of the DOD UCR and that have been approved for inclusion in the DOD UCR by the UC steering group.

c. When submitting a product for DOD UC APL fast track consideration—

(1) The same sponsorship and product documentation rules apply for DOD UC APL fast track products (see para 3–1).

(2) For products that are being presented as a new DOD UCR product category or subcategory, that category will be specified at the time of submission into the APL Integrated Tracking System (APLITS).

(3) If there are existing test results or certifications available, include them in the APLITS product documentation submission.

(4) Once the documentation package is complete, a meeting will be scheduled with the vendor, sponsors, UCCO, JITC, distributed laboratory (if applicable), and network services engineering team to evaluate product maturity, features affecting assured service, and suitability for DOD UC APL testing.

(5) The UC steering group will provide guidance and issue resolution as necessary.

(6) UCCO will disseminate the results of the meeting and related discussions and clarify the way forward to all parties.

3–4. Army sponsor duties

The Army sponsor must ensure that critical testing requirements and all findings identified during cybersecurity testing are properly documented. The Army sponsor must also assist with mitigation strategies for these findings. An analysis of each finding must be conducted to determine its impact to the overall security posture of the system under test. The Army sponsor must—

a. Request a sponsor account via APLITS for each point of contact (a minimum of two are required).

b. Accept sponsorship designation for the product offering.

c. Assist DISA with developing requirements for the desired product and product features.

d. Ensure the acquisition of UC products aligns with DOD policy and direction.

e. Attend the ICMs.

f. Attend the cybersecurity and interoperability out-briefs to discuss test results and, if applicable, assist with mitigation strategies and POA&Ms.

g. Coordinate all testing activities and logistics with UCCO and vendors.

h. Provide to the vendor any STIGs and security readiness review checklists that are not publicly available.

i. Coordinate with the DOD test facility for funding by the Government sponsor or vendor.

3–5. Vendor duties

The vendor must—

a. Request a vendor account via APLITS.

b. Download and review the DOD UC APL Process Guide (http://www.disa.mil/network-services/ucco).

c. Submit documentation in accordance with the DOD UC APL Process Guide.

d. Apply relevant STIG requirements to the submitted product and submit results to UCCO.

e. Ensure onsite engineering support is provided during all phases of DOD UC APL testing assigned for the solution under test.

f. Attend the ICMs and out-briefs to discuss test results and, if applicable, assist with mitigation strategies and the POA&M.

g. Provide deployment guidelines for the solution under test to UCCO.

h. Coordinate all testing activities and logistics with UCCO and Government sponsors.

i. Assist testing centers in development of test plans and test procedures.

Appendix A

References

Section I

Required Publications

AR 25–1
Information Management Army Information Technology (Cited in para 2–1.)

AR 25–2
Army Cybersecurity (Cited in para 1–1.)

DOD UC APL Process Guide
DOD Unified Capabilities Approved Products List Process Guide (Cited in para 3–1*a*.) (Available at http://www.disa.mil/)

DODI 8100.04
Unified Capabilities (UC) (Cited in para 1–1.)

UCR 2013, Change 1
DOD Unified Capabilities Requirements 2013, Change 1, June 2015(Cited in para 1–5*a*.) (Available at http://disa.mil/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 25–30
Army Publishing Program

Committee on National Security Systems Instruction 4009
Committee on National Security Systems (CNSS) Glossary (Available at https://www.cnss.gov/.)

Committee on National Security Systems Policy (CNSSP) 11
Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, 10 June 2013 (Available at https://www.cnss.gov/.)

FIPS 140–2
Cryptographic Modules (Available at http://csrc.nist.gov/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil/).

DA Form 2028
Recommended Changes to Publications and Blank Forms

Glossary

Section I

Abbreviations

AO
authorizing official

APL
Approved Products List

APLITS
Approved Products List Integrated Tracking System

AR
Army regulation

CA
certification authority

CHESS
Computer Hardware and Enterprise Software Solutions

CIO/G–6
Chief Information Officer, G–6

CNSSI
Committee on National Security Systems instruction

DA
Department of the Army

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODI
Department of Defense instruction

FIPS
Federal Information Processing Standards

IA
Information Assurance

ICM
initial contact meeting

JITC
Joint Interoperability Test Command

NIAP
National Information Assurance Partnership

NIST
National Institute of Standards and Technology

POA&M
plan of action and milestones

STIG
Security Technical Implementation Guide

UC
Unified Capabilities

UCCO
Unified Capabilities Certification Office

UCR
Unified Capabilities Requirements

Section II

Terms

Cybersecurity product (formerly known as Information Assurance product)
A product whose primary purpose is to provide security services (for example, confidentiality, authentication, integrity, access control, and nonrepudiation of data), correct known vulnerabilities, and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks (CNSSI No. 4009). Note: DODI 8500.01 has transitioned from the term information assurance to the term cybersecurity. This could potentially impact cybersecurity-related terms

Cybersecurity tools
Cybersecurity tools, previously called Information Assurance tools, are a category of cybersecurity devices that are not yet fully defined. These devices must meet the cybersecurity requirements for DOD systems as defined in UCR 2013, Change 1. Functional requirements will be added in future versions of the document.

Cybersecurity–enabled product (formerly known as Information Assurance–enabled product)
A product or technology whose primary role is not security but provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, multifunctional devices and security-enabled messaging systems (CNSSI No. 4009). Note: DODI 8500.01 has transitioned from the term Information Assurance to the term cybersecurity. This could potentially impact cybersecurity-related terms.

Section III

Special Abbreviations and Terms
This section contains no entries.